Indiana Office of Technology

Information Security Policies
& Minimum Compliance Requirements

Prepared for:

Indiana State Government

Effective Date:
July 1, 2005

Information Security Policies
& Minimum Compliance Requirements

Prepared for

Indiana State Government

Prepared by the Information Security Working Group

Joe Hunt
Ronald Baker
Deb Barrick
Suzanne Flynn
Cindy Hochgesang
Jim McQuiston
John Richard
Jim Rudolph
Kathee Saylor
Larry Smith
Jim Welsh

Table of Contents

1.0 Information Security Policy Introduction

1.1 Overview and Purpose

The purpose of this document is to establish minimum information security policies for Indiana state government.[1] The document also establishes minimum compliance activities to implement the information security policies included in Section 4. These policies apply to all hardware, software, data, information, network, personal computing devices, support personnel, and users within State Agencies. Hereinafter, this coverage will be referred to as the "Information Resources."

Data is critical to the continued workings of state government, as state government collects, analyzes, uses, and maintains large amounts of information to carry out its required duties. The public rightly assumes and should be assured that the data in the possession of state government is secure and protected from unauthorized access and modification.

All Workforce Members are responsible for protecting Information Resources. Generally, data in the possession of state government is public record subject to public disclosure unless that data is specifically exempted from disclosure by law. ***These policies apply to <u>all</u> data, regardless of public availability.***

These Information Security Policies and Minimum Compliance Requirements are written with the purpose of reinforcing the following important concepts:

- Ensuring the confidentiality, integrity of information, and availability of Information Resources is a critical function of state government.
- Recognizing that information security reflects a "business of government" need and not just a technology need.
- Establishing a core understanding that Workforce Members share accountability for information security.
- Promoting the appropriate balance of security risk levels and cost of risk mitigation and disaster recovery.
- Promoting an enterprise-wide understanding of, and responsibility for, information security.
- Ensuring information security requirements include both in-house and outsourced resources.
- Establishing formal processes for reviewing and approving individual waivers and policy exceptions before those waivers or exceptions may be implemented.

[1] The Judicial Department and Legislative Department are not in the purview of the State Chief Information Officer, but are encouraged to adopt these policies.

1.2 Information Security Policy Principles

Technology systems and their network connectivity offer significant benefits in collecting, analyzing, storing, using, and sharing information. But, along with the benefits, comes the need to safeguard Information Resources from damage, originating both internally and externally, and from threats possibly originating from malicious intent or inadvertent activities. Security safeguards, if ignored, could have disastrous results for unprepared sites.

State Agency information systems make extensive use of interconnected computers and databases. Security challenges arise with the interconnectedness of systems, complexity of host configurations, vulnerabilities introduced in the software development process, and a variety of other factors. These all contribute to making unprepared sites open to unwanted activity and related problems.

It is the intent of these Information Security Policies and Minimum Compliance Requirements to assist Workforce Members in all of state government in protecting Information Resources they use or manage from unauthorized access, modification, damage, or destruction. ***These policies define the minimum requirements approach to information security for State Agencies. Compliance is mandatory.***

1.3 ***De Minimis*** Use

While the State expects that Information Resources shall be primarily used to achieve the State's business goals and objectives, it also recognizes that its Workforce Members occasionally need to use Information Resources for personal reasons that (i) cannot reasonably be handled away from work or (ii) are, in the private business sector, generally permitted in the workplace. Personal use, therefore, is inextricably linked to these security policies because personal use—perhaps even more so than business use—is likely to subject Information Resources to potential security vulnerabilities.

The Information Resources Use Agreement (IRUA) permits limited, or "*de minimis,*" personal use of Information Resources by Workforce Members, which is in accord with the State Ethics Commission's policy. The IRUA (along with additional resources noted below) seeks to promote an enterprise-wide understanding of appropriate use of Information Resources and to provide Workforce Members reasonable safe harbor from ethics violation concerns.

As a result, some personal use of Information Resources is permitted as long as the Workforce Member's work product does not, in the opinion of the Workforce Member's supervisor, suffer. For example, permissible uses include:

- placing personal appointments and contact information in electronic calendars and address books;
- sending and receiving personal Email through a Web-based Email client that has been pre-approved by the CISO or the CISO's designee; and,

- browsing appropriate Web sites online.

Under no circumstances, of course, are Information Resources to be used for the viewing or circulation of obscene, offensive, or discriminatory material; for outside commercial gain; for political activity; or to damage or compromise the security of the State or its Information Resources.

It should be noted, however, that any document "created, received, retained, maintained, or filed" is public record according to the Access to Public Records Act, IC 5-14-3. Further, the State reserves the right to monitor all use of Information Resources and to enforce penalties up to immediate termination for inappropriate use. Thus, there is no so-called "right to privacy" when engaging in *de minimis* personal use of Information Resources.

More examples of appropriate use and frequently asked questions can be found online at iot.in.gov/security . Workforce Members shall not be considered to have violated ethics rules for *de minimis* personal use of Information Resources consistent with the IRUA, unless the Workforce Member's State Agency adopts a stricter policy of its own.

1.4 Scope of the Information Security Policies

These policies apply to all Workforce Members and cover any Information Resources.

1.5 Organization of the Information Security Policies

The Information Security Policies and Minimum Compliance Requirements include the following sections:

- Policy Statement
- Policy Objective
- Policy and Control Requirements
  - Compliant Activities
  - Permitted Activities
  - Prohibited Activities
- Exceptions to Policy
- Policy Violations and Disciplinary Actions
- Implementation Responsibility
- Compliance Responsibility
- References

Each section either includes a statement of policy or provides guidance on the needed activities or actions to comply with the policy and the party responsible to ensure compliance.

2.0 Information Security Policy Establishment, Approval, Exceptions, and Enforcement

2.1 Information Security Policy Establishment

The authority to establish information security policies is given to the State Chief Information Officer (CIO) under Indiana Code 4-13.1-2-2(a)-10. The CIO has established the Chief Information Security Officer (CISO) position and delegated authority for the development and enforcement of approved information security policies.

2.2 Information Security Policy Approval

To be effective, any policy must be consistent with other existing directives, laws, organizational culture, guidelines, procedures, and the organization's overall mission. With these objectives in mind, it is the policy of IOT to periodically review these information security policies for comparison with best practices in information security and to update the policies to meet the changes in technologies, personnel, and sound business practices. Changes to these policies shall be prepared by the CISO or designee for approval by the CIO.

2.3 Information Security Policy Exceptions

These information security policies include consideration of the need for waivers or variances based upon unique legislative or business requirements. Any request for an individual waiver and policy exception shall be submitted to, and subject to the approval of, the CISO or the CISO's designee before the waiver or exception may be implemented.

2.4 Information Security Policy Enforcement

The Information Security Policies prohibit unauthorized access to its Information Resources. The State reserves the right to monitor the use of Information Resources. Individuals found to be in violation of these policies may face disciplinary actions up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

3. Information Security Policy Implementation

3.1 Information Security Policy Implementation Overview

The CISO and CIO shall take steps to communicate these policies to all State Agency heads. State Agency heads are required to introduce these policies into the operations of their agencies in a manner that ensures and communicates management's support for the policies and requires Workforce Member compliance. These policies will serve as the vehicle for emphasizing the State's commitment to information security and for establishing clear expectations for Workforce Member performance, behavior, and accountability.

3.2 Information Security Policy Implementation Actions

Each State Agency shall assign one Workforce Member the responsibility of information security oversight within the agency and to coordinate and ensure agency compliance of information security with the CISO.

3.2a State Agencies with Current Information Security Policies:

The following actions are required from State Agencies with information security policies in place:

A. Review these Information Security Policies.
B. Compare with existing agency policies.
C. Identify differences between agency policies and these Information Security Policies.
D. Where there are differences, prepare information for agency Workforce Members on needed changes in information security policies and expectations to follow these Information Security Policies.
E. If there are differences that conflict with required information security policies for the agency, complete the following:
    1. Document the difference(s) between the policies.
    2. Document legislative, contractual, and/or other mandatory requirements for the agency's current policies.
    3. Submit a written request to the CISO via the Help Desk for exception to these Information Security Policies.
        a. If approved, inform agency Workforce Members of new information security policies in place for the agency.
        b. If not approved, inform agency Workforce Members of changes in information security policies.

3.2b The following actions are required from State Agencies with no information security policies in effect:

A. Review these Information Security Policies.
B. Inform agency Workforce Members about these Information Security Policies.

Any questions or requests for assistance shall be directed to the CISO via the Help Desk.

4. Information Security Policies and Minimum Compliance Requirements

Indiana Office of Technology Information Systems Security Policy **Appropriate Use**	POLICY # 4.1	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 3
	TITLE:	Appropriate Use		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.1.1 Policy Statement:

Information Resources shall be used in an appropriate and legal fashion and shall be limited to authorized purposes.

4.1.2 Policy Objective:

Ensure that Information Resources are efficiently used for their intended purposes.

4.1.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Information Resources shall be used for business purposes.
  - A Workforce Member leaving a workstation shall first ensure that the workstation is properly secured from unauthorized access.
  - A Workforce Member shall access information only in a manner consistent with approved methods of system access and entry.
  - A Workforce Member shall take care to use Information Resources in an ethical and legal manner and in ways that do not adversely affect the State, his or her State Agency, or Information Resources.
  - All information contained on state computers or developed while on the job using state facilities or resources shall be the exclusive property of the State.
  - Only equipment or software properly procured, licensed, or being evaluated by the State shall be used.
  - Only authorized IT staff shall install software/hardware on state-owned equipment.
  - At all times, the Workforce Member shall make all reasonable efforts to protect and keep software strictly confidential in accordance with the license or any other agreement executed by the State.
  - Licensed software being used or evaluated by the State shall comply with the vendor license agreement.
  - Internet access shall be used for legitimate business purposes.

- **Permitted Activities:**
  - If permitted by a *de minimis* use policy, as discussed in Section 1.3, Information Resources may be used occasionally and minimally for personal use in emergencies and for personal activities that cannot be reasonably managed outside the workplace. These situations might include communicating with schools, child-care providers, physicians, and other similar activities.
  - Information Resources may be used for authorized training activities.
  - In those cases of authorized personal use:
    - The duration of personal use shall be short and infrequent.
    - The Workforce Member shall use personal time, unless it is not reasonably practical.
- Software developed by or for the State Agency may be shared with prior written approval from the appropriate State Agency head or designee.

- **Prohibited Activities:**
  - At no time shall a Workforce Member transmit obscene or harassing messages.
  - At no time shall a Workforce Member access pornographic, sexually explicit, or obscene material.
  - At no time shall a Workforce Member use state resources for outside fund-raising, to participate in lobbying, or for partisan activity.
  - At no time shall a Workforce Member attempt to circulate chain letters or solicitations to purchase or sell items.
  - At no time shall a Workforce Member use state resources for the purpose of conducting outside commercial activities or in support of other "for-profit" activities, *e.g.*, outside employment or businesses.

4.1.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted by the CISO:

- With prior approval, other Workforce Members may be authorized to install software/hardware on State-owned equipment.
- With prior written approval, the use of personal or third-party equipment and/or software at State facilities may be allowed.

4.1.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the

act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.1.6 Implementation Responsibility:

State Agencies are required to inform Workforce Members of appropriate use of Information Resources.

4.1.7 Compliance Responsibility:

All Workforce Members shall be responsible for appropriate use of Information Resources.

State Agencies shall be responsible for implementing and enforcing the Appropriate Use Policy within their supported areas.

State Agency security staff reserve the right to monitor use of Information Resources.

4.1.8 References:

HIPAA 164.310 (b) Workstation Use
(c) Workstation Security

Indiana Office of Technology Information Systems Security Policy **Security Awareness and Training**	POLICY # 4.2	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 3
	TITLE:	Security Awareness and Training		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.2.1 Policy Statement:

Workforce Members shall be trained on the Information Security Policies and information security issues.

4.2.2 Policy Objective:

Ensure that all Workforce Members are aware of their information security responsibilities and how to fulfill those responsibilities.

4.2.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Each State Agency shall participate in the Information Security awareness and training programs to ensure that all Workforce Members are aware of their security responsibilities and understand how to fulfill those responsibilities.
  - Workforce Members shall attend an approved Information Security Awareness Training within 30 days of being granted access to any Information Resources (in some cases, they may be required to attend training before being granted access).

All Workforce Members shall receive periodic updates, training, and supporting reference materials regarding information security to allow them to properly protect Information Resources.

Each State Agency shall maintain documentation of the information security training provided to Workforce Members and the State's PeopleSoft HR application.

4.2.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- Cases of a temporary or short duration access to Information Resources (*e.g.*, physical access for the purpose of replacing hardware components) would require training only on the relevant parts of the Information Security Policies.

4.2.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.2.6 Implementation Responsibility:

The IOT shall develop an Information Security Policies awareness and training program for use by State Agencies.

Each State Agency shall supplement the IOT information security training to meet agency-specific requirements.

4.2.7 Compliance Responsibility:

The CISO or designee shall be responsible for implementing and enforcing this Security Awareness and Training Policy.

Executive management within each State Agency shall be responsible for ensuring compliance with the Security Awareness and Training Policy.

Security personnel (security program managers and security officers) shall be responsible for serving as expert consultants for their agency.

System owners shall be responsible for identifying unique issues and security requirements applicable to the systems they manage.

System administrators and IT support personnel who have been entrusted with a high degree of authority over support operations critical to a successful security program shall receive additional awareness and technical training.

4.2.8 References:

HIPAA 164.308 (a) (5) (i) Security Awareness and Training
(ii) Implementation Specifications
(A) Security Reminders
(B) Protection from Malicious software
(C) Log-in monitoring
(D) Password management

NIST 800-53

Indiana Office of Technology Information Systems Security Policy **Personnel Security**	POLICY # 4.3	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 3
	TITLE:	Personnel Security		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.3.1 Policy Statement:

Workforce Members shall comply with the Information Security Policies.

4.3.2 Policy Objective:

Reduce the risks of human error, theft, fraud, or misuse of Information Resources.

4.3.3 Policy and Control Requirements:

- **Compliant Activities:**
  - All managers and supervisors shall promote compliance with these Information Security Policies.
  - Each Workforce Member shall have a job description that includes requirements to comply with these policies.
  - Managers and supervisors shall monitor Workforce Members' compliance with these policies.
  - Each Workforce Member shall sign an Information Resources Use Agreement that documents that the Workforce Member has received the Information Security Policies, has been briefed on compliance with policies, and that the Workforce Member understands and agrees to comply with these policies.
  - Each State Agency shall provide periodic information security awareness training to Workforce Members.
  - Before a Workforce Member is granted access to Information Resources, the individual shall undergo a background check that complies with the IOT's and the Indiana State Personnel Department requirements. The results of the background check shall be documented and included in the Workforce Member's personnel file.
  - A Workforce Member changing job functions shall be oriented to changes in information security requirements for the new job functions and additional personal screening required by the job function. The orientation and background check shall be documented in the Workforce Member's personnel file.
  - State Agencies shall have documented procedures for the timely removal of terminated Workforce Members from access to Information Resources.

- State Agencies shall have documented procedures for the review and reclassification of appropriate security levels for Workforce Members whose duties have changed due to promotion, demotion, or reassignment.

4.3.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- Temporary access to Information Resources based on special needs.

4.3.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.3.6 Implementation Responsibility:

The IOT shall develop an information security orientation program for Workforce Members.

State Personnel shall maintain background check requirements for all Workforce Members.

Each State Agency shall maintain records of the following:

- Documentation of the background checks.
- Workforce Members' signed Information Resource Use Agreements.
- Periodic information security awareness training attendance.

4.3.7 Compliance Responsibility:

State Agencies shall be responsible for implementing and enforcing the Personnel Security Policy within their supported areas.

Managers and supervisors are responsible for promoting and ensuring compliance with these policies.

Each State Agency is responsible for ensuring that its Workforce Members receive information regarding these Information Security Policies as part of the orientation for new Workforce Members and upon reemployment.

Each State Agency is responsible for ensuring that no Workforce Member accesses Information Resources until an Information Resource Use Agreement is signed.

4.3.8 References:

HIPAA 164.308 (a) (3) (i) Workforce Security
(ii) Implementation Specifications
(A) Authorization or Supervision
(B) Workforce Clearance Procedure
(C) Termination Procedures

State Personnel Department Background Checks for State Employment

Cross-reference Security Awareness and Training

Indiana Office of Technology Information Systems Security Policy **Password Security**	POLICY # 4.4	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 3
	TITLE:	Password Security		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.4.1 Policy Statement:

Workforce Members accessing Information Resources who use password authentication shall use a password that complies with this policy.

4.4.2 Policy Objective:

Ensure that Information Resources are protected by passwords that are secure and selected to hinder unauthorized access to password-protected resources.

4.4.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Each Workforce Member shall have a unique user identification (User-ID) and password.
  - Workforce Members shall assign their own passwords.
  - Passwords shall be changed (at least) every 90 days.
  - Passwords shall contain a minimum of 8 characters.
  - Passwords shall include a combination of at least 3 of the following 4 types: alphabetic, numeric, special characters, both upper and lower case.
  - Passwords shall be changed after first assignment or following a password reset.
  - Passwords shall be encrypted while stored on the computer.
  - Passwords shall be changed as soon as they expire.
  - Accounts shall be locked out after three unsuccessful login attempts.
  - Passwords shall not be duplicated within the last 13 occurrences (changes).
  - Workforce Members shall change passwords when advised of a potential security breach by the CISO or agency information security officer.

- **Permitted Activities:**
  - Password defaults can be used for initial hardware and software setup or configuration. Following initial activities, these defaults shall be changed.
  - Expired passwords shall be used only to reset or to self-assign a new password.

- **Prohibited Activities:**
  - Passwords shall not contain the User-ID, user name, company name, replicated sequence of characters, or any complete dictionary words.
  - Passwords and User-IDs shall not be provided to others or shared.
  - Passwords and User-IDs shall not be posted or displayed where other individuals may have access.

4.4.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- Passwords for special use and restricted accounts such as training or service accounts may be defined to not expire, shared, etc.
- Passwords may be included in secured batch files only if no other acceptable alternative can be identified.
- Password complexity requirements may be adjusted to suit older legacy hardware and software in instances where meeting the full requirements of this policy would either be impossible or cost-prohibitive.

4.4.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.4.6 Implementation Responsibility:

Each Workforce Member shall be responsible for selecting a secure password, maintaining password confidentiality, and promptly changing the password when any security breach is suspected. The responsible business or IT owner shall review security logs regularly to identify suspicious login attempts or recurring failures.

Any individual requesting a Workforce Member's password shall be referred to this policy document, the agency security officer, or to the CISO or the CISO's designee.

4.4.7 Compliance Responsibility:

State Agencies shall be responsible for implementing and enforcing the Password Security Policy within their supported areas.

State Agency supervisors shall be responsible for ensuring that Workforce Members who report to them comply with this policy.

4.4.8 References:

HIPAA 164.310 Physical Safeguards
(c) Workstation Security
HIPAA 164.312 Technical Safeguards
(a) (1) Access Control
(2) Implementation Specifications
(i) Unique User Identification
(ii) Emergency Access Procedure
(iii) Automatic Logoff
HIPAA 164.312 (d) Person or Entity Authentication
Cross-reference Access Security Policy

Indiana Office of Technology Information Systems Security Policy **Email Usage**	POLICY # 4.5	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 4
	TITLE:	Email Usage		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.5.1 Policy Statement:

Email resources shall be used in a proper and professional manner and for authorized purposes.

4.5.2 Policy Objective:

Ensure the efficient use of state Email resources and to provide for the availability and stability of those state Email resources.

4.5.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Workforce Members shall use state-provided Email services only for legal and permitted activities.
  - Workforce Members shall understand that Email messages are public records and, therefore, are open to public disclosure.
  - Workforce Members shall only open, forward, or respond to Emails from recognized sources for acceptable or business-approved purposes.
  - Any Workforce Member who distributes confidential, personally identifying, or sensitive information using Email, shall take steps to ensure that the information is secure from disclosure by using IOT approved methods.
  - All provisions of State and federal law shall be adhered to in the transmission of confidential, personally identifying, or sensitive information as well as all provisions of published agency policy and this Email Usage Policy.
  - All Email messages shall be treated in the same manner as their paper equivalents, *i.e.*, all Email messages are subject to the individual records retention guidelines of the agency and any retention policies dictated by State and federal law.
  - A Workforce Member receiving inordinate amounts of non-business Email shall report the occurrence to the appropriate help desk for action.

- **Permitted Activities:**
  - Workforce Members may use Email for non-business purposes in compliance with a *de minimis* use policy as discussed in Section 1.3.

- Workforce Members may view personal Email through a Web-based Email serviced approved by the CISO or CISO-designee.
- The use of Internet-based instant messaging (IM) programs (MSN Messenger, Yahoo Messenger, Internet Relay Chat [IRC], Jabber, AOL Instant Messaging [AIM], etc.) shall be permitted only with formal approval by the CISO or the CISO's designee.

- **Prohibited Activities:**
  - Workforce Members shall not send any Email that is illegal (*e.g.*, copyright violations, personal identity information, obscene information, or for fraudulent purposes), harassing, or threatening.
  - Workforce Members shall not knowingly forward or respond to unsolicited external commercial Email, commonly referred to as SPAM, while utilizing State resources. All Email users shall delete Emails of this type immediately upon receipt. Inordinate amounts of SPAM shall be reported to the Help Desk for proper control measures.
  - Workforce Members shall not knowingly forward or respond to Emails that are chain letters, pyramid selling schemes, or multi-level marketing schemes while utilizing State resources. Emails of this type shall be immediately deleted upon receipt.
  - Workforce Members shall not utilize State resources to knowingly send Email that makes use of forged headers and/or FROM addresses that are not in the control of the State.
  - Workforce Members shall not send Email messages that could be reasonably considered as disruptive to another's work.
  - Workforce Members shall not send a high volume of Emails to render the State's Email resources unusable (such as to cause a denial of service attack).
  - Workforce Members shall not subscribe another individual to mailing lists without the other individual's approval.
  - Workforce Members shall not allow any other person or third party to utilize state Email resources or to resell or make any commercial use of these resources.
  - Workforce Members shall not download personal Email.

4.5.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- Use of IOT-approved instant messaging services.
- Possible use of Email for mass mailings for business-approved purposes.

4.5.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.5.6 Implementation Responsibility:

Workforce Members shall be responsible for appropriate use of Information Resources.

An Email account is afforded to Workforce Members for use in conducting official state business. These Email resources are a privilege and not a right. As such, Workforce Members are required to use the Email in a proper and professional manner.

Request to use Internet instant messaging for external communication should be directed to the CISO via IOT's help desk.

4.5.7 Compliance Responsibility:

It is the responsibility of all Workforce Members to adhere to this Email Usage Policy. Any Workforce Member needing clarification or interpretation of this policy shall seek guidance from their agency's IT contact or from the IOT via the IOT's help desk.

Workforce Members shall understand that Email messages are public records and open to public disclosure.

All messages sent by state electronic mail resources are considered state records.

The State reserves the right to access, monitor, and disclose all messages sent over its Email system for any purpose. The State may also disclose Email messages to law enforcement officials without prior notice to the individuals who may have sent or received such messages.

The IOT has the responsibility of enforcing these guidelines and ensuring that the State's Email resources remain available and in good working order.

4.5.8 References:

HIPAA 164.312 (e) (1) Transmission Security.
(2) (i) Integrity controls
(ii) Encryption

Cross-reference Records Management Policy

Indiana Office of Technology Information Systems Security Policy **Virus Control**	POLICY # 4.6	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 3
	TITLE:	Virus Control		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.6.1 Policy Statement:

All devices connected to the state network shall be actively protected from viruses and other malicious software.

4.6.2 Policy Objective:

Protect the Information Resources from potential losses resulting from computer viruses and other malicious software. Within this policy, the term "virus" means any virus, worm, Trojan horse, or other malicious software.

4.6.3 Policy and Control Requirements:

- **Compliant Activities:**
  - All devices such as workstations, desktops, laptops, and servers that connect to the state network shall have virus protection software installed, activated, and updated.
  - State Agencies shall develop and implement a plan to provide for the acquisition, deployment, and recurrent updating of their virus protection software for all devices.
  - State Agencies shall make available to Workforce Members training materials on the effective use of virus protection software.
  - Each calendar year, the senior executive responsible for information technology within each State Agency shall provide written assurance to the CISO or the CISO's designee that the State Agency has complied with this Virus Control Policy.
  - Anti-virus software shall be updated on, at least, a weekly basis to ensure that the latest virus definition files are installed.
  - Anti-virus software shall be configured to scan the boot record for viruses automatically on startup.
  - All removable storage devices or media shall be scanned for viruses each time the device or media is connected to the state network.
  - Devices that connect from outside the state firewall shall have virus protection that meets or exceeds the state standard.
  - All Workforce Members shall comply with IOT or individual State Agency virus alert messages and comply with any remediation measures.

- **Prohibited Activities:**
  - No executable files shall be downloaded from Post Office Protocol Version 3 (POP3) or Simple Mail Transfer Protocol (SMTP) accounts.
  - No Workforce Member may disable virus protection software.

4.6.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Virus protection software may be disabled temporarily by IT staff or at the direction of the IT staff if required to install application software or to perform other system maintenance functions.

4.6.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.6.6 Implementation Responsibility:

All Workforce Members controlling devices that are connected to the state network are subject to this policy.

4.6.7 Compliance Responsibility:

The senior executive responsible for information technology within each State Agency is responsible for ensuring that this policy is applied to all devices under the control of the agency and attached to the state network.

The IOT is responsible for acquiring and applying network management tools necessary to detect any virus attempting to gain access through the State's firewall and to exclude that virus.

The IOT or State Agency IT staff members are responsible for acquiring and applying network management tools necessary to detect any virus within the State's firewall and to contain that virus within a specific segment of the state network.

All Workforce Members are responsible for assuring anti-virus software is installed and updated on any device that they control. Further, they are also responsible for immediately reporting to the appropriate help desk any indication that a virus is present on a device they control that is, or may be, connected to the state network.

4.6.8 References:

HIPAA 164.312 (c) (1) Integrity

Indiana Office of Technology Information Systems Security Policy **Data Categorization**	POLICY # 4.7	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Data Categorization		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.7.1 Policy Statement:

All state data shall be categorized based on the need for availability and level of confidentiality.

4.7.2 Policy Objective:

Establish the appropriate requirements for security and management of data.

4.7.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Data owners shall categorize all data under their control according to the following Categorization Matrix:

		Confidentiality			
		Confidential	**Sensitive**	**Private**	**Public**
Availability	**Critical** 24/7/365				
	Necessary Can be down for up to a week.				
	Non-critical Can be down for more then a week				

  - State Agencies shall coordinate with the IOT and agency Workforce Members to provide security appropriate for the data categorization.

4.7.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

4.7.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.7.6 Implementation Responsibility:

Data owners shall categorize their data according to the above Categorization Matrix. These categorizations shall be reviewed on a regular basis and updated as necessary.

The IOT is responsible for establishing data categorization standards and procedures.

The IOT is responsible for implementing security procedures to protect data based on the data's categorization.

4.7.7 Compliance Responsibility:

The IOT and the State Agencies shall be responsible for implementing and enforcing this policy within their supported areas.

4.7.8 References:

HIPAA 164.308 Administrative Safeguards
(a) (7) (i) Contingency plan.
(ii) Implementation specifications:
(E) Applications and data criticality analysis

IC 6-8.1-7-1 Confidentiality
Internal Revenue Code Sections 6103 and 7213 Federal prohibitions against tax return information
IC 4-1-10 (effective July 1, 2005) State Agency disclosure of Social Security Numbers
IC 5-14 Indiana Public Records Law

Indiana Office of Technology Information Systems Security Policy **Physical Security**	POLICY # 4.8	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Physical Security		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.8.1 Policy Statement:

Physical access to Information Resources shall be restricted to the minimum number of individuals needing access to those resources.

4.8.2 Policy Objective:

Prevent unauthorized access, damage, and interference to Information Resources.

4.8.3 Policy and Control Requirements:

- **Compliant Activities:**
  - State data processing and communications areas shall be protected by physical controls appropriate for the size and complexity of the operations and the categorization of data maintained in those locations.
  - State Agencies shall ensure that access to restricted areas and information is limited to authorized Workforce Members.
  - Visitors shall be escorted at all times.
  - State Agencies shall ensure that their Workforce Members have only the appropriate level of access for the completion of their job responsibilities.
  - Workforce Members and visitors shall wear state-issued identification at all times when on state premises.
  - State Agencies shall establish physical security standards, including controlling and storing, for tape files, CDs, diskettes, and other media to prevent unauthorized use or removal from state facilities.

4.8.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted by the CISO:

- Temporary access may be granted to Workforce Members requiring additional access to Information Resources for special projects, overtime, etc., provided that

the timely return to normal access is completed upon the conclusion of the project.

- Temporary access may be granted to vendors or support personnel for completion of a state-initiated project.

4.8.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action, up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.8.6 Implementation Responsibility:

The IOT and State Agencies are responsible for determining the appropriate physical security for Information Resources under their control.

4.8.7 Compliance Responsibility:

State Agencies shall be responsible for implementing and enforcing the Physical Security Policy within their supported areas including documenting maintenance activities relating to physical security.

Supervisors shall be responsible for ensuring that their Workforce Members comply with this policy.

Indiana Department of Administration (IDOA) has responsibility for building security.

4.8.8 References:

HIPAA 164.310 Physical Safeguards

(a) (1) Facility Access Controls

(2) Implementation Specifications

(i) Contingency Operations

(ii) Facility Security Plan

(iii) Access Control and Validation Procedures

(iv) Maintenance Records

Indiana Office of Technology Information Systems Security Policy **Data Management**	POLICY # 4.9	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Data Management		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.9.1 Policy Statement:

All information collected or maintained by State Agencies shall be secured according to the data's categorization.

4.9.2 Policy Objective:

Protect the data and information that State Agencies collect or maintain from loss, alteration, mutilation, destruction, or release to unauthorized individuals.

4.9.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Data and Information Resources shall have an identified business owner responsible for the integrity and safeguard of the resources.
  - All data in the control of a State Agency shall be assigned a category and documented according to the Data Categorization Policy.
  - Data shall be protected through backup and storage to ensure safety, security, and recoverability based on the data categorization.
  - All Workforce Members shall ensure that the distribution of, release of, or access to State Agency reports, data, and files are consistent with the data categorization.
  - Those processes where data can be changed or otherwise manipulated shall be designed to ensure that the integrity and accuracy of the data are maintained according to the categorization of the data.
  - Any unauthorized access to data shall be reported in an incident report to the CISO or the CISO's designee.

- **Prohibited Activities:**
  - Use of Social Security Numbers (SSN) in information system programs and projects is prohibited unless specifically authorized under federal or State law.

4.9.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

4.9.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.9.6 Implementation Responsibility:

All Workforce Members controlling data and systems residing on the State network or resources are responsible for the implementation of this policy.

4.9.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing the Data Management Policy within their supported areas.

The IOT and State Agency security staff reserve the right to monitor use of all state-provided Information Resources.

Supervisors shall be responsible for ensuring that their Workforce Members comply with this policy.

4.9.8 References:

HIPAA 164.308 (a) (4) (i) Information Access Management
(ii) Implementation Specifications
(A) Isolating Health Care Clearinghouse Functions
(B) Access Authorization
(C) Access Establishment and Modification
HIPAA 164.308 (a) (6) (i) Security incident procedures.
(ii) Implementation specification: Response and Reporting
HIPAA 164.310 (d) (1) Device and Media Controls
(2) Implementation Specifications
(iv) Data Backup and Storage
HIPAA 164.312 (c) (1) Integrity
Cross-reference Data Categorization Policy

Indiana Office of Technology Information Systems Security Policy **Copyright and Software Protection**	POLICY # 4.10	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Copyright and Software Protection		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.10.1 Policy Statement:

Workforce Members are required to comply with the U.S. Copyright Law, nondisclosure, and vendor licensing agreements governing the installation, use, and distribution of software used by State Agencies.

4.10.2 Policy Objective:

Ensure that State Agencies are in compliance with software license agreements.

4.10.3 Policy and Control Requirements:

- **Compliant Activities:**
  - The IOT shall conduct regular audits to ensure that terms of software licenses are met.
  - All contracts with external information system service providers (including facilities management arrangements) shall clearly state that it is the responsibility of the service provider to ensure that appropriate licenses are held by the service provider for any product used to provide the service.
  - Each State Agency shall maintain an inventory of all software and related licenses used by the agency.
  - Software shall only be installed by an authorized IT staff member.
  - Any software developed by a Workforce Member using state resources remains the property of the State and may only be released with authorization from the CIO.

- **Permitted Activities:**
  - Any deviation from the normal copyright agreement may be made with the permission of the copyright holder.

- **Prohibited Activities:**
  - The unauthorized copying, installation, or distribution of any software.

4.10.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

4.10.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.10.6 Implementation Responsibility:

The IOT and State Agencies are responsible for implementation and enforcement of this policy.

4.10.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing this policy within their supported areas.

The IOT and State Agency security staff reserve the right to monitor use of all State-provided Information Resources.

4.10.8 References:

U.S. Copyright Law

Indiana Office of Technology Information Systems Security Policy **Media and Data Destruction**	POLICY # 4.11	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 5
	TITLE:	Media and Data Destruction		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.11.1 Policy Statement:

State Agency data storage devices and printed media shall be disposed of in a manner consistent with the security categorization of the information contained on these devices or media.

4.11.2 Policy Objective:

Ensure the secure disposition of physical and electronic information along with the hardware and electronic media on which it is stored.

4.11.3 Policy and Control Requirements:

- **Compliant Activities:**
  - All data and programs shall be removed from electronic storage media by State Agencies before sending the storage media to Indiana Department of Administration, Surplus Division (State Surplus) moving to another agency, exchanging with a vendor while under warranty, donating, and/or destroying.
  - State Agencies shall maintain a log that provides an audit trail of destruction or disposition of the device.
  - The method used for removal of data depends upon the operability of the device:
    - Operable hard drives that will be reused shall be overwritten prior to disposition.
    - If the operable hard drive is to be removed from service completely, it shall be physically destroyed or degaussed.
    - If the hard drive is inoperable, has reached the end of its useful life, or cannot be properly overwritten, then it shall be physically destroyed or degaussed.
  - Acceptable methods of removing data are: Overwriting, Degaussing, and Physical Destruction.

- **Overwriting**
  - When overwriting data, the data shall be properly overwritten with a pattern that complies with the Department of Defense (DOD) standard 5220.22-M.
  - Removal of state data is not considered complete until three overwrite passes and a full verification pass have been completed.
  - The software used shall have the capability to overwrite the entire disk drive, independent of any Basic Input/Output System (BIOS) or firmware capacity limitation, making it impossible to recover any meaningful data.
  - The software shall have the capability to overwrite using a minimum of three cycles of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium.
  - The software shall have a method to verify that all data has been removed.
  - Sectors not overwritten shall be identified.

- **Degaussing**
  - When degaussing any media, the product manufacturer's directions shall be carefully followed. It is essential to determine the appropriate rate of coercively (magnetic saturation) for degaussing.
  - Shielding materials (cabinets, mounting brackets) that may interfere with the degausser's magnetic field shall be removed from the hard drive before degaussing.
  - Hard disk platters shall be in a horizontal direction during the degaussing process.

- **Physical Destruction**
  - Hard drives shall be destroyed when they are defective, cannot be repaired, or when State data cannot be removed for reuse.
  - Physical destruction shall be accomplished to an extent that precludes any possible further use of the hard drive. This can be achieved by removing the hard drive from the cabinet, removing any steel shielding materials and/or mounting brackets, and cutting the electrical connection to the hard drive unit. The hard drive shall then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle, or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.
  - Drilling multiple holes into the hard disk platters is another method of destruction that will preclude use of the hard drive and provide *reasonable* protection against unauthorized retrieval of the data written on the drive.

Removal of State Data/Programs from Other Electronic Devices:

- Electronic devices that hold user data or configurations in volatile memory shall have all State data removed by either the removal of the battery or electricity supporting the volatile memory or by such other method recommended by the manufacturer for devices where the battery is not removable. This is to include all computer equipment that has memory such as personal computers, Personal Digital Assistants (PDA), routers, firewalls and switches.

Removal of State Data/Programs from Other Computer Media"

- If there is any risk of disclosure of confidential or sensitive data on media other than computer hard drives, that media shall be destroyed. Disintegration, incineration, pulverization, shredding, or melting is an acceptable means of destruction. Examples of other media include but are not limited to tapes, diskettes, CDs, DVDs, Write Once/Read Many (WORM) devices, and Universal Serial Bus (USB) data storage devices.

Certification of the Removal of State Data/Programs from Surplus Computer Hard Drives and Electronic Media"

- Each State Agency shall establish and use an audit procedure to ensure compliance with standards.
- Prior to submitting surplus forms to the agency's appropriate organizational unit, the process for removal of State data shall be documented on a form or file that explicitly outlines:
  - The methods (Overwrite, Degauss, and Destruction) used to expunge the data from the storage media.
  - The make and model of equipment that was released for surplus from which State data was removed.
  - The state inventory ID.
  - The serial number of the personal computer or other equipment.
  - The name of the person responsible for the removal of state data.

The completed form/file (containing the following information) shall be maintained in a central location, by each State Agency, for audit purposes.

Method of Sanitation	Make and Model of Equipment	State ID Number	Serial Number	Name of Person Who Performed the Sanitation/Destruction

When sending equipment to State Surplus, a label shall be affixed to the equipment to denote that the information has been removed.

See the sample label below.

Storage media has been sanitized per IOT media destruction policy Date ____/_____/_____ Technician: _____

- **Prohibited Activities:**
  - The disposal of storage media without removal of the data with an approved method.
  - Deleting files does not normally remove information from storage media. Since the delete process does not prevent data from being recovered by technical means, it is **not** an acceptable method of removing state data from State Agency-owned hard disks or other storage media.

4.11.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

4.11.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.11.6 Implementation Responsibility:

IOT shall establish and maintain guidance regarding acceptable methods for destruction of media and removal of data.

Each State Agency is responsible for auditing the removal of State data for compliance with this standard when any computer hard drive or electronic media are released for surplus, transferred, traded in, disposed of, or the hard drive is being replaced. The State Agency shall ensure that the audit process occurs in a timely manner, and that the audit controls are effective.

4.11.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing the Media and Data Destruction Policy within their supported areas.

4.11.8 References:

Department of Defense (DOD) standard 5220.22-M.

HIPAA 164.310 (d) (1) Device and Media Controls
(2) Implementation Specifications
(i) Disposal
(ii) Media Reuse
(iii) Accountability

Cross-reference Asset Management

Indiana Office of Technology Information Systems Security Policy **Asset Tracking**	POLICY # 4.12	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Asset Tracking		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.12.1 Policy Statement:

State Agencies shall track and assign accountability for state-owned Information Resources.

4.12.2 Policy Objective:

Protect Information Resources from theft or loss and to govern the receipt, surplus, and movement of these items throughout state government.

4.12.3 Policy and Control Requirements:

- **Compliant Activities:**
  - State Agencies shall use the State PeopleSoft Financial Management System to comply with this policy.
  - State Agencies shall log Information Resources information at the time of receipt and assign accountability of the resource.
  - State Agencies shall log the relocation, transfer, surplus, or disposition of Information Resources.

- **Permitted Activities:**
  - State Agencies may use other software or processes to supplement asset tracking.

4.12.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Exceptions to the State Asset Management Policy may only be granted by the State Board of Accounts or the Auditor's Office.

4.12.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.12.6 Implementation Responsibility:

State Agencies.

4.12.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing this policy within their supported areas.

Overall monitoring of compliance is the responsibility of the State Board of Accounts and the Auditor's Office.

4.12.8 Regulatory References:

HIPAA 164.310 Physical Safeguards
(d) (1) Device and Media Controls

Accounting Manual for State Agencies (www.in.gov/sboa)
Cross-reference Media and Data Destruction

Indiana Office of Technology Information Systems Security Policy **Access Security**	POLICY # 4.13	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Access Security		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.13.1 Policy Statement:

Information Resources shall be configured and maintained to ensure availability only to authorized and authenticated Workforce Members.

4.13.2 Policy Objective:

Minimize the potential exposure to state assets to damage from unauthorized use and the loss of sensitive or confidential data, damage to public trust, or damage to critical Information Resources.

4.13.3 Policy and Control Requirements:

- **Compliant Activities:**
  - The IOT shall have a documented procedure for reviewing the authorization level and ensuring the configuration of Information Resources to ensure availability only to authorized Workforce Members.
  - State Agencies shall have documented procedures for requesting, authorizing, granting, enabling, and periodically reviewing access to Information Resources.
  - Access to Information Resources shall be authorized by State Agency security coordinators and/or business owners taking into account the following:
    - Data categorization,
    - Business need,
    - Potential conflict with segregation of duties or incompatible job functions.
  - When enforceable, Workforce Members shall ensure that workstations are locked or logged off after 10 minutes of inactivity.

4.13.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- Emergency access rights to vendors for support purposes.
- The use of system utilities and devices capable of bypassing system access security shall only be permitted with formal approval from the CISO or the CISO's designee.

4.13.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.13.6 Implementation Responsibility:

The IOT shall establish procedures for configuring and maintaining Information Resources to support authorized access.

4.13.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing the Access Security Policy within their supported areas.

The IOT and State Agency security staff reserve the right to monitor use of all state-provided Information Resources.

4.13.8 References:

HIPAA 164.308 (a) (4) (i) Information Access Management
(ii) Implementation Specifications
(A) Isolating Health Care Clearinghouse Functions
(B) Access Authorization
(C) Access Establishment and Modification

Indiana Office of Technology Information Systems Security Policy **Network Security**	POLICY # 4.14	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 3
	TITLE:	Network Security		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.14.1 Policy Statement:

All state network resources, regardless of the platform on which they reside or where they are located (mainframe, departmental distributed systems, or personal computers), shall be monitored to ensure that all network changes and network users are properly authorized.

4.14.2 Policy Objective:

Protect the state network and their services from unauthorized access, modification, destruction, or disclosure.

4.14.3 Policy and Control Requirements:

- **Compliant Activities:**
  - All central cabling and associated facilities shall be kept either in a computer room environment or, where this is not feasible, in a locked room or closet.
  - Access to this equipment shall be restricted to specific personnel.
  - Network analyzers and data scopes shall be stored securely and their use strictly controlled.
  - Network configuration information shall be maintained and the network logs compared to this information to identify unrecognized devices. Any identified devices shall be reported as a cyber security incident.
  - When a new network connection is about to be installed on the state network, the person or department ordering the service shall be contacted to verify that this is an authorized connection.
  - Adequate schematics of network cabling and server locations shall be maintained. Schematics shall include physical location and the person(s) responsible for any servers.
  - Any changes to network or server configurations shall be processed in accordance with change control procedures.
  - Network operating software shall ensure that when user sessions terminate, either normally or abnormally, all related network sessions are also terminated.
  - All remote network access using dial-in services shall be through an IOT approved modem pool.

- All remote network access using broadband services shall use IOT-authorized Virtual Private Network (VPN) services.

- **Permitted Activities:**
  - Non-state computer systems may be permitted to connect to the state network if they are authorized and conform to the Information Security Policies.
  - Only IOT-authorized Workforce Members shall be permitted to download, install, or run security programs or utilities that test and monitor the security of the system (password cracking programs, packet sniffers, network mapping tools, or port scanners).

- **Prohibited Activities:**
  - Workforce Members shall not add to or alter the state network without approval from the CISO or the CISO's designee.
  - Workforce Members inside the firewall shall not be connected to the state network and another network at the same time (*e.g.*, using a modem to connect to an external network while logged into the state network).
  - Workforce Members shall not modify the network configurations provided.

4.14.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- Connecting to the state network and a second network by a modem or other device for authorized business purposes.

4.14.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.14.6 Implementation Responsibility:

The IOT is responsible for the state network and for providing the following services:

- Establish and maintain, including patch management, a secure state network.
- Develop and publish Information Technology Security Architecture.
- Develop and maintain incident response procedures.
- Adherence to statewide information security policies and procedures on any devices they manage.

- Design and maintain a secure state WAN by controlling the setup and use of network routers and switches.
- Develop and maintain incident response procedures.
- Allocate, register, and centrally manage networking addresses for the supported protocols.

4.14.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing the Network Security Policy within their supported areas.

The IOT and the State Agency security staff reserve the right to monitor use of all state-provided Information Resources.

The IOT is responsible for the following activities:

- Installation of monitoring and/or intrusion detection/prevention tools on the network.
- Actively monitoring to assure continued operation and that physical access and configuration changes are authorized.
- Develop, maintain, and enforce the state Enterprise Security roles, policies, standards, audits, and business process reviews.
- Develop, maintain, and monitor network security roles, policies, standards, tools, and procedures.
- Design and maintain a secure state network by monitoring network traffic for potential intrusion detection.
- Control the setup and use of network firewalls, routers, and switches.
- Investigate and report attack incidents on the campus area and metropolitan area networks.
- Determine trusted and non-trusted networks on the state Intranet and Extranet.
- Ensure that only properly authorized persons are allowed to connect devices to the state network.

4.14.8 References:

IC 4-13.1 Indiana Office of Technology

Indiana Office of Technology Information Systems Security Policy **Remote Access**	POLICY # 4.15	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 3
	TITLE:	Remote Access		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.15.1 Policy Statement:

Any remote access into the state network shall be authorized and use approved resources and methods.

4.15.2 Policy Objective:

Protect the state network from unauthorized access, modification, destruction, or disclosure.

4.15.3 Policy and Control Requirements:

- **Compliant Activities:**
  - All remote access connections shall be made for conducting state business and work-related activities.
  - All use of remote access connections shall comply with the State's Appropriate Use policy.
  - All Workforce Member connections to the state network for the purposes of remote access shall be made through IOT provided and approved resources and methods.
  - All personal computers connected to the state network via remote access shall have virus protection equivalent to, or exceeding, state standards.
  - All remote access connections made by personal computer shall be protected by a personal firewall that meets or exceeds the state standard.
  - All remote access users shall limit their connections to the minimum time needed to complete the necessary tasks and shall terminate their connections promptly after use.
  - All remote access users shall ensure that personal computers are properly secured from unauthorized access.
  - State Agencies shall have documented procedures for the timely removal of terminated Workforce Members from access to Information Resources.
  - State Agencies shall have documented procedures for the review and reclassification of appropriate security levels for Workforce Members whose duties have changed due to promotion, demotion, or reassignment.

- **Prohibited Activities:**
  - Remote access points not approved by IOT such as inbound analog modem lines, wireless access points (WAP), or any other transport medium not under the control of the State is prohibited.
  - Remote Workforce Members shall not be connected to the state network and another network at the same time (*e.g.*, using a modem or other option to connect to an external network while logged into the state network).
  - Any form of network bridging, without the approval of IOT, for the purpose of remote access is prohibited.
  - Workforce Members shall not alter the settings and properties of the remote access connection provided by IOT.

4.15.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

4.15.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.15.6 Implementation Responsibility:

The IOT shall establish and publish the standards and methods for remote access to the state network.

4.15.7 Compliance Responsibility:

The IOT, State Agencies, and Workforce Members shall be responsible for implementing and enforcing this policy within their supported areas.

State Agencies shall determine which of their Workforce Members shall be granted remote access and periodically review that access.

4.15.8 References:

Cross-reference Appropriate Use
Cross-reference Network Security
Cross-reference Virus Protection
Cross-reference Firewall Security

Indiana Office of Technology Information Systems Security Policy **Encryption Use**	POLICY # 4.16	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Encryption Use		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.16.1 Policy Statement:

State Agencies shall use an encryption algorithm to protect data according to the data's categorization.

4.16.2 Policy Objective:

Protect the State's confidential data resources from unauthorized access, destruction, or modification.

4.16.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Data to be encrypted shall be encrypted using an IOT-approved encryption algorithm.
  - Encrypted State data shall be decrypted only for use by authorized Workforce Members.
  - All data classified as confidential shall be stored in encrypted format regardless of the media on which it resides.

- **Prohibited Activities:**
  - Storage or transmission of confidential data in clear text or any other unencrypted open or proprietary format is prohibited.
  - Decryption keys, tokens, or any other decryption device shall not be stored with the media or data that is encrypted.

4.16.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- Where end-point to end-point encryption cannot be achieved, the data shall be transmitted using IOT-approved secure protocol.

4.16.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.16.6 Implementation Responsibility:

The IOT shall establish the standards, methods, and resources for encryption of confidential data.

4.16.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing the Encryption Use Policy within their supported areas.

The IOT and State Agency security staff reserve the right to monitor use of all state-provided Information Resources.

A State Agency shall ensure that confidential data in the agency's possession are encrypted.

4.16.8 Regulatory References:

Advanced Encryption Standard (AES) algorithm per the NIST FIPS-197
RFC 2406
NIST FIPS-197
IC 6-8.1-7-1 Confidentiality
HIPAA 164.312 Technical Safeguards
(a) (1) Access Control
(2) Implementation Specification
(iv) Encryption and Description

Indiana Office of Technology Information Systems Security Policy **Applications Security**	POLICY # 4.17	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Applications Security		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.17.1 Policy Statement:

All applications developed by or purchased for State Agencies shall be designed and implemented in accordance with these security policies.

4.17.2 Policy Objective:

Ensure that information security is integrated into the development of every application.

4.17.3 Policy and Control Requirements:

- **Compliant Activities:**
  - The evaluation of any application purchased shall include an assessment of its security compliance and risks.
  - All application security vulnerabilities shall be corrected promptly.
  - Each State Agency shall establish security requirements for each aspect of the agency's applications development methodology.
  - The security requirements for applications developed by State Agencies shall be based on the categorization of data supported by the application.
  - The security requirements for applications developed by State Agencies shall be based on the risk assessment prepared by each agency.

4.17.4 Exceptions to Policy:

Exceptions to this policy may be granted only by the CISO or the CISO's designee.

4.17.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.17.6 Implementation Responsibility:

The CISO or the CISO's designee shall establish minimum standards for mandatory contract language regarding information security.

The CISO or the CISO's designee shall establish minimum requirements regarding information security in application development.

State Agencies shall develop and report application security requirements to the CISO or the CISO's designee.

4.17.7 Compliance Responsibility:

The IOT shall be responsible for developing guidance for including security issues in applications development.

The IOT and State Agency security staff reserve the right to monitor compliance with this policy.

4.17.8 References:

Cross-reference Data Categorization

Indiana Office of Technology Information Systems Security Policy **Records Management**	POLICY # 4.18	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Records Management		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.18.1 Policy Statement:

State Agencies shall use and follow an effective records management process.

4.18.2 Policy Objective:

Ensure the proper handling, storage, retrieval, and destruction of public records to support public access to documents, both hard copy and electronic copy, generated or used by the State.

4.18.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Each State Agency shall develop, document, and implement a Records Management Program to cover information in both hard copy and electronic copy.
  - State Agency records management programs shall comply with Indiana Code 5-14 and seek to comply with guidance from the Indiana Commission on Public Records.
  - Each State Agency shall document compliance with the agency's records management program.

4.18.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Exceptions to public records management may be granted only by the Indiana Commission on Public Records.

4.18.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.18.6 Implementation Responsibility:

All Workforce Members who create, store, retrieve, use, or destroy public records are responsible for compliance.

State Agencies are responsible for establishing records management practices that comply with this policy.

4.18.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing the Records Management Policy within their supported areas.

The Indiana Commission on Public Records is responsible for ensuring compliance with Indiana laws on records management.

4.18.8 References:

Indiana Code 5-14
Cross-reference Data Categorization
Cross-reference Media and Data Destruction

Indiana Office of Technology Information Systems Security Policy **Cyber Incident Reporting**	POLICY # 4.19	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 4
	TITLE:	Cyber Incident Reporting		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.19.1 Policy Statement:

State Agencies shall report cyber security incidents to the CISO or the CISO's designee.

4.19.2 Policy Objective:

Coordinate activities among State Agencies experiencing cyber security incidents and gain the benefits of quicker identification and resolution to protect Information Resources.

4.19.3 Policy and Control Requirements:

A cyber security incident is considered to be any adverse event that threatens the confidentiality, integrity, or accessibility of Information Resources. These events include but are not limited to the following malicious activities:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data.
- Unwanted disruption or denial of service of Information Resources.
- Unauthorized use of a system for the transmission, processing, or storage of data.
- Changes to system hardware, firmware, or software characteristics without the State Agency's knowledge, instruction, or consent.
- Attempts to cause failures in critical infrastructure services or the loss of critical supervisory or data acquisition systems.
- Attempts to cause failures that may result in loss of life or have a significant impact on the health or economic security of the State.

- **Compliant Activities:**
  - **Urgent Incidents**
    - Workforce Members shall report the following types of incidents to the Help Desk by calling (317) 232-3251 *as close to the time of discovery as possible*.
      - Widespread damaging virus or worm infections.

- Major outages due to denial of service attacks.
- Mission-critical application failures.
- Attacks on mission-critical infrastructure services.
- Unauthorized root or administrator access to critical servers, routers, firewalls, etc.
- Major reconnaissance scans and probes.

- **Non-urgent Incidents**
  - Workforce Members shall report the following types of incidents to the Help Desk at (317) 232-3251 *by the end of the next business day*.
    - Suspected unauthorized access.
    - Attempted but unsuccessful denial of service attacks.
    - Degradation of service attacks.

- **Prohibited Activities:**
  - Disclosing information regarding reported incidents with anyone other than the State reporting structure.
  - Reporting individual incidents to any law enforcement agency without written permission of the CISO or the CISO's designee.

4.19.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

4.19.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.19.6 Implementation Responsibility:

All Workforce Members are expected to observe and actively support the activities identified in this Cyber Incident Reporting Policy.

The CISO or the CISO's designee is responsible for submitting incident reports to the CIO. The CISO or the CISO's designee shall validate reports before action is taken.

Incident reports shall contain as much of the following information as is available at that particular time. Additional information such as the resource costs for handling the incident may not be known initially but are included here as a reminder that this information shall be tracked and reported in a follow-up report.

Contact Information

- Name
- Organization name
- Email address
- Phone number(s)

Description of Incident

- Date and time incident was detected
- Date and time incident actually occurred (if different from above)
- Type of incident (*e.g.*, Web defacement, virus/worm)
- Method of intrusion (*e.g.*, vulnerability exploited)
- Level of unauthorized access (*e.g.*, root, administrator, user)
- Log extracts if appropriate
- Any other relevant information

Affected System(s)

- Internet Protocol (IP) address and hostname
- Purpose of the system (*e.g.*, DNS server, router, Email server, XZY application server)
- Operating systems, software versions, and patch levels
- The type of protection that is in place (*e.g.*, firewall, Intrusion Detection System [IDS] or anti-virus make, model, and version)

Attack Source(s)

- IP address and hostname
- Internal or external source

Damage Assessment (estimated)

- Impact of attack on business
- Staff time to detect, handle, and recover from the incident
- Costs due to information loss, downtime, etc.

4.19.7 Compliance Responsibility:

The IOT shall be responsible for reporting:

- Information about prior incidents with other State Agencies.
- Acts of terrorism to the Director of the Indiana Department of Homeland Security (IDHS) where mandated by law.

IDS systems shall be checked on a periodic basis for proper function and configuration.

Where extraordinary circumstances prevent obtaining prior consent from the CISO or the CISO's designee, the State Agency information security officer may make the report to other State Agencies, the IDHS, or law enforcement agencies.

In the case where the State CISO is not permitted to make the report for reasons of security or due to a request from an investigating authority, a State Agency information security officer may make the report.

4.19.8 References:

HIPAA 164.308 Administrative Safeguards
(a) (6) (i) Security incident procedures.
(ii) Implementation specification: Response and Reporting

Cyber Security Policy ITP04-01 Incident Report Policy

Indiana Office of Technology Information Systems Security Policy **Auditing and Logging**	POLICY # 4.20	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 3
	TITLE:	Auditing and Logging		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.20.1 Policy Statement:

The use of Information Resources shall be audited based on the categorization of those resources.

4.20.2 Policy Objective:

Protect state records from loss, destruction, and falsification.

4.20.3 Policy and Control Requirements:

- **Compliant Activities:**
  - System auditing shall be enabled on Information Resources to capture the event logs.
  - Operating system and application software logging shall be enabled on all hosts and servers.
  - Alarm and alert functions shall be enabled as appropriate.
  - Audit trail logs and programs/utilities shall be accessible only by security staff and or other authorized individuals.
  - All system administrators shall have their activities logged and reviewed on a regular basis.
  - Unsuccessful login attempts shall be logged and reviewed on a regular basis.
  - Each entry in the audit log shall contain at least the following information: Username or User-ID, date and time, terminal ID, error level (success or failure), and event description.
  - All machines shall have their clocks synchronized to guarantee the validity of audit log timestamps.
  - Logs shall be stored on a secured resource and retained based on data categorization or retention schedule.

- **Prohibited Activities:**
  - Logs shall not contain non-encrypted passwords.

4.20.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee. Any exception shall be reduced to writing, documenting the reason for the exception, the benefits and risks for the exception, and the specific devices and time period for which the exception is granted.

4.20.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.20.6 Implementation Responsibility:

The IOT shall ensure that auditing and logging functions are enabled and operational.

4.20.7 Compliance Responsibility:

The IOT security team and State Agency security staff shall be responsible for the following activities:

- Audit logs shall be reviewed from the perimeter access control systems on a daily schedule.
- Audit logs for servers and hosts on the internal, protected network shall be reviewed on a weekly schedule.
- Audit logs for mission-critical servers and hosts on the internal protected network shall be reviewed on a daily schedule.
- System integrity checks of firewalls and other network perimeter access control systems shall be performed on, at least, a monthly basis.
- All trouble reports received by system administration personnel shall be reviewed for symptoms that might indicate intrusive activity.
- All trouble reports shall be reviewed by system administration personnel for symptoms that may indicate intrusive activity.
- The tracking of inappropriate computer use shall be documented when requested by management.
- Report any suspicious activities or patterns detected through the auditing process to the appropriate State Agencies.

4.20.8 References:

HIPAA 164.308 (a) (1) (i) Security Management Process
(ii) Implementation Specifications
(D) Information Systems Activity Review
HIPAA 164.312 (b) Audit Controls
(c) (1) Integrity
(2) Mechanism to authenticate electronic protected health information
Cross-reference Cyber Incident Reporting

Indiana Office of Technology Information Systems Security Policy **Firewall Security**	POLICY # 4.21	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Firewall Security		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.21.1 Policy Statement:

The state network shall be secured with firewall protection and services.

4.21.2 Policy Objective:

Reduce and contain the risk to the state network from unauthorized access, modifications, destruction, or disclosure.

4.21.3 Policy and Control Requirements:

- **Compliant Activities:**
  - The state firewall structure shall be operated only by trained personnel with an approved background check.
  - All firewall configuration and implementation criteria shall be documented and filed in a secure location.
  - Changes to the firewall shall be requested and approved utilizing the firewall Change Request Form.
  - Sub-networks shall be separately protected by firewalls where appropriate based on the data categorization.
  - Firewalls shall be periodically subjected to penetration tests and audits.

4.21.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the State Chief Information Security Officer (CISO) or designee.

4.21.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.21.6 Implementation Responsibility:

The IOT shall provide and maintain firewall protection as required by this policy.

4.21.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing the Firewall Security Policy within their supported areas.

The IOT and State Agency security staff reserve the right to monitor use of state-provided Information Resources.

4.21.8 References:

Cross-reference Data Categorization

Indiana Office of Technology Information Systems Security Policy **Wireless Security**	POLICY # 4.22	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Wireless Security		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.22.1 Policy Statement:

All wireless connections shall meet state standards for authorization, authentication, and secure communication.

4.22.2 Policy Objective:

Protect Information Resources from unauthorized access through wireless network connection.

4.22.3 Policy and Control Requirements:

- **Compliant Activities:**
  - All wireless networking equipment (*e.g.*, Access Points, NIC Cards, etc.) connected to the State network shall be registered and approved by the CISO or the CISO's designee prior to connection.
  - Access Points shall be periodically subjected to penetration tests and audits.
  - All wireless implementations shall be configured and operated in accordance with IOT Wireless Implementation Guidelines.

- **Prohibited Activities:**
  - Installation and operation of unauthorized wireless implementations are strictly prohibited.

4.22.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

4.22.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.22.6 Implementation Responsibility:

The CISO or the CISO's designee shall establish and update standards regarding wireless implementations for the state network.

All Workforce Members controlling or operating wireless devices connected to the state network shall ensure that those wireless devices are registered with the CISO or the CISO's designee prior to connection to the network.

4.22.7 Compliance Responsibility:

The IOT and State Agencies shall be responsible for implementing and enforcing the Wireless Security Policy within their supported areas.

The IOT and State Agency security staff reserve the right to monitor use of state-provided Information Resources.

4.22.8 References:

IOT Wireless Network policy (ITP 04-01).

Indiana Office of Technology Information Systems Security Policy **Risk Assessment**	POLICY # 4.23	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 2
	TITLE:	Risk Assessment		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.23.1 Policy Statement:

Each State Agency shall periodically assess risks to Information Resources under the State Agency's control.

4.23.2 Policy Objective:

Ensure that State Agencies have an understanding of their risk exposures and the opportunity to plan mitigation actions in order to minimize the probability and impact of damage to Information Resources.

4.23.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Each State Agency shall conduct and document a risk assessment in compliance with IOT standards for Information Resources in the agency's control.
  - Each State Agency shall develop and implement a risk mitigation plan to address identified risks.
  - Each State Agency shall submit the risk assessment and risk mitigation plans to the CISO or the CISO's designee for review and acceptance.
  - State Agency assessments and plans shall be updated at least every two years or as needed to address the risk to Information Resources including:
    - When changing existing systems.
    - When business processes change.
    - When specific areas of concern are identified.

4.23.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- State Agencies with minimal risk exposure may request permission to update their risk assessment and mitigation plans on a schedule different from every two years.

4.23.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.23.6 Implementation Responsibility:

The IOT in cooperation with State Agencies shall be responsible for:

- Establishing minimum standards for conducting and documenting the risk assessments.
- Establishing minimum standards for preparing the risk mitigation plans.

4.23.7 Compliance Responsibility:

The IOT shall review State Agency risk assessments and mitigation plans for acceptability.

4.23.8 References:

HIPAA 164.308 Administrative Safeguards
(a) (1) (i) Security Management Process
(ii) Implementation Specifications
(A) Risk Analysis
(B) Risk Management

NIST 800-53

Indiana Office of Technology Information Systems Security Policy **Disaster Recovery**	POLICY # 4.24	ISSUED 7/01/05	LAST REVISED 7/01/05	PAGE 1 of 3
	TITLE:	Disaster Recovery		
	AUTHOR:	Information Security Working Group		
	POLICY APPROVAL DATE:			

4.24.1 Policy Statement:

The IOT, in cooperation with each State Agency shall establish a Disaster Recovery and Business Continuity Plan based on business needs and risk assessment.

4.24.2 Policy Objective:

Ensure that State Agencies can recover their Information Resources in a timely fashion following a disaster.

4.24.3 Policy and Control Requirements:

- **Compliant Activities:**
  - Each State Agency shall develop a Disaster Recovery and Business Continuity Plan based on IOT standards and the agency's risk assessment and mitigation plan.
  - Each State Agency shall submit the Disaster Recovery and Business Continuity Plan to the CISO or the CISO's designee for review and acceptance.
  - Each State Agency shall test its Disaster Recovery and Business Continuity Plan on regular intervals to identify needed improvements and ensure that the plan can be implemented effectively and timely.
  - State Agency Disaster Recovery and Business Continuity Plans shall be updated, at least, every two years or as needed to address risks to Information Resources including:
    - When changing existing systems.
    - When business processes change.
    - When specific areas of concern are identified.

4.24.4 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- State Agencies with minimal risk exposure may request permission to update their Disaster Recovery and Business Continuity Plans on a schedule different from every two years.

4.24.5 Policy Violations and Disciplinary Actions:

A Workforce Member found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

4.24.6 Implementation Responsibility:

The IOT, in cooperation with the State Agencies, shall be responsible for:

- Establishing minimum standards for Disaster Recovery and Business Continuity Plans.
- Establishing minimum standards for testing Disaster Recovery and Business Continuity Plans.

State Agencies shall complete, submit, and test a Disaster Recovery and Business Continuity Plan.

4.24.7 Compliance Responsibility:

The IOT shall review each State Agency's Disaster Recovery and Business Continuity Plans for acceptability and consistency with other plans.

4.24.8 References:

HIPAA 164.308 Administrative Safeguards
(a) (7) (i) Contingency plan.
(ii) Implementation specifications:
(A) Data backup plan
(B) Disaster recovery plan
(C) Emergency mode operation plan
(D) Testing and revision procedures
(8) Evaluation

Executive Order 05-09
Cross-reference Risk Assessment
Cross-reference Data Categorization

Definitions

	Abuse	Unauthorized use of information, resources, or facilities
	Access	Authorized to create, view, update, or delete programs
	Access Control	The enforcement of specific authorization rules based on positive identification of users and the systems or data they are permitted to access.
	Active Scan	Attempts to exploit discovered vulnerabilities.
	Application(s)	A program designed to assist in the performance of a specific task, such as word processing, accounting, or inventory management.
	Audit Trail	A record showing who accessed a computer system or network resource and what operations were performed during a given period of time. OR In reference to computing, a means of tracing all activities affecting a piece of information, such as a data record, from the time it is entered into a system to the time it is removed. An audit trail makes it possible to document, for example, who made changes to a particular record and when.
	Authentication	The process of identifying a Workforce Member based on login information. Authentication merely ensures that the Workforce Member is who he or she claims to be but says nothing about the Workforce Member's access rights.
	Authorization	A right granted an individual to use an information resource. Authorization is typically set up by a system administrator and verified by the computer based on some form of user identification, such as a code number or password.
	Authorized User	Employees or contractors, who have written approval to develop computer systems, maintain or use specific resources.
	Availability Levels (used for Data Categorization)	State data is categorized based on three (3) levels of *AVAILABILITY* and four (4) levels of *CONFIDENTIALITY*. The ***AVAILABILITY*** levels are defined as follows: • Critical – Data needs to be available seven days / week and 24 hours / day. Any loss of access is critical. • Necessary – Data can be down or not available for up to one (1) week. • Non-Critical – Data can be down or not available for longer than one (1) week.
	Benchmark	A test used to compare performance of hardware and/or software.
BIOS	Basic Input/Output System	The basic input/output system built into computers that controls the operation of disk drives, displays, and keyboards, as well as serial and parallel communications (modems, printers).
CAN	Campus Area Network	An environment in which users are spread out over a broad area as in universities, hospitals, and governmental facilities. There may be several local area networks (LAN) on a CAN.

CIO	Chief Information Officer	An officer of a business responsible for its computers and information technology. Used throughout to refer to the Chief Information Officer of the State, unless specifically noted.
CISO	Chief Information Security Officer	An officer of a business responsible for identifying and implementing information security policies and procedures. Used throughout to refer to the Chief Information Security Officer of the State, unless specifically noted.
CISM	Certified Information Security Manager	A certification to ensure executive management that those earning the designation have the required knowledge and ability to provide effective security management and consulting.
CISSP	Certification for Information System Security Professional	A certification reflecting the qualifications of information systems security practitioners.
	Confidential Data	Data that is available to any State employee or contractor having a direct or indirect State interest therein. Data used within a State Agency, or division of a State Agency, that is specified for management and control purposes in performance of assigned responsibilities. An example of confidential information would be software documentation.
	Confidentiality Levels (used for Data Categorization)	State data is categorized based on three (3) levels of *AVAILABILITY* and four (4) levels of *CONFIDENTIALITY*. The ***CONFIDENTIALITY*** levels are defined as follows: • Confidential – Data with the highest level of security and protection. The unauthorized loss or disclosure of this information could pose a risk to the State or individual that it references. • Sensitive – Data that requires special precautions to ensure the integrity and protection from unauthorized modification or deletion. • Private – Data that is not for public use, control, or participation. This information can be thought of as belonging to an individual rather than the general public. • Public – Data with the lowest level of security and protection. This information can be generally viewed by anyone with minimum controls to ensure integrity.
	Contractor	Anyone with information access to programs and/or data who is not an Indiana State government employee.
	Critical Resource	That resource determined by the State Agency management and agency head to be essential to the agency's critical mission and functions, the loss of which would have a severe impact. This would include applications, systems, data, load, or hardware components
	Data	A collection of concepts and program instructions for manual or automated processing. OR Used in reference to a collection of information that can be used for automated processing to make calculations and decisions.
	Degaussing	The process of removing magnetism from a device. Normally a procedure that uses a strong magnetic field to erase or alter the magnetic orientation of another device. Once degaussed, the disk drive will contain no information or files.

DMZ	Demilitarized Zone	A computer or small sub-network that sits between a trusted internal network, such as a corporate private LAN, and an un-trusted external network, such as the public Internet.
	De minimis	Limited or proscribed use.
	Disclosure	Unauthorized access to confidential or sensitive data.
	Exposure	Vulnerability to loss resulting from accidental or intentional disclosure, modification, or destruction of information assets.
	General Public Data	Data that is maintained specifically for general publication and use by the public or general user community. Examples would include telephone directories, help screens, global Email messages, etc.
HIPAA	Health Insurance Portability and Accountability Act	The federal law that defines requirements for health information security.
IAC	Indiana Administrative Code	Rules promulgated to implement provisions of the Indiana Code .
IC	Indiana Code	Statutes enacted.
	Information Assets	Data resident on a computer, magnetic medium, paper files, or another storage medium that is used by the agency(ies) to support normal business functions.
IOT	Indiana Office of Technology	State Agency authorized under IC 4-13.1 with responsibilities for Information Resources.
IP	Internet Protocol	Specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source. IP by itself is akin to the postal system in that it allows you to address a package and drop it in the system, but there is no direct link between you and the recipient. On the other hand, TCP/IP establishes a connection between two hosts so they can send messages back and forth for a period of time.
ISDN	Integrated Services Digital Network	International communications standard for sending voice, video, and data over digital telephone lines or normal analog telephone wires. ISDN supports data transfer rates of 64 Kbps. Most ISDN lines offered by telephone companies provide two lines at once, called B channels. One line can be used for voice and the other for data, or both can be used for data to provide data rates of 128 Kbps.
ISP	Internet Service Provider	A company that provides access to the Internet.
	Information Resources	The hardware, software, data, information, network, personal computing devices, support personnel, and users connected to, used in, located in, or within State Agencies.
IT	Information Technology	The broad subject concerned with all aspects of managing and processing information, especially within a large organization or company.
ISO 17799	International Organization for Standardization	A code of practice for information security management.

LAN	Local Area Network	A short distance data communications network used to link computers and peripheral devices under a form of standard control. The connecting of computers housed within a given area (usually a building) allows for the sharing of common files, printers, and applications.
	Malicious Software	Software designed specifically to damage or disrupt a computer system.
NIST	National Institute of Standards and Technology	Formed in 1901 as the National Bureau of Standards, NIST is part of the U.S. Department of Commerce. NIST works with industry and government to advance measurement science and to develop standards in support of industry, commerce, scientific institutions, and all branches of government.
	Network	Computer networks connect all types of computers and computer related devices–terminals, printers, modems, servers, mainframes desktop computers, etc. OR A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communication links.
	Node	A computer or some other device, such as a printer connected to a network. A point of connection into a network.
	Non-volatile memory	Type of memory used in a computer system that retains its contents when power is turned off (or interrupted).
	Owner	An individual primarily responsible for the creation and/or maintenance of specific information.
	Passive Scan	Means of listening without making our presence known.
	Password	A protected word or string of characters that is known to only one person that serves as evidence of the person's identity to gain access to computer systems.
	Penetration Testing	Testing that shows the consequences of compromise and weaknesses not discovered through scanning.
PDA	Personal Digital Assistant	Handheld device that combines computing, telephone and/or fax and networking features. A typical PDA can function as a cellular phone, fax sender, and personal organizer. Some Web applications on *AccessIndiana* can be performed on a PDA.
	Personally Identifying Information	Information that specifically identifies an individual or a fact about an individual.
POP3	Post Office Protocol Version 3	POP3 is a protocol widely used on the Internet or other IP-based networks to retrieve electronic mail from a (typically distant) Email server.
PDF	Portable Document Format	PDF captures formatting information from a variety of desktop publishing applications, making it possible to send formatted documents and have them appear on the recipient's monitor or printer as the sender intended.

	Private	Not available for public use, control, or participation. Belonging to a particular person or persons, as opposed to the public or the government.
	Resources	Information, equipment, and controls to manage data processed by a computer system or network.
	Restricted Public	Most data that is currently defined as "Public Records". This data is not suitable for unconnected display but should be made readily available through a simple request and approval process. An example of restricted public data would be public employee salaries.
	Risk	The probability that a particular security threat will exploit a particular vulnerability.
	Risk Assessment	An analysis that examines an organization's Information Resources, its existing controls, and its remaining organization and computer system vulnerabilities. It combines the loss potential for each resource or combination of resources with an estimated rate of occurrence to establish a potential level of damage in dollars or other assets.
	Secret	Data that is specifically controlled by statute (Tax Returns), data that is secret or of a particularly sensitive nature (investigatory files), or other data that affects the operation and security of computers (passwords).
	Security Controls	Hardware, programs, procedures, policies, and physical safeguards which are put in place to assure the integrity and protection of data processing assets.
	Security Tools	Suite of tools that enables security testing/verification of network, servers and desktops.
	Segregation of Duties	The concept of ensuring that no one individual is in the position that enables him/her to perpetuate or conceal errors or irregularities in the normal course of his authorized duties.
	Sensitive Data	Information that requires special precautions to ensure the integrity of the information by protecting it from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness. Examples of sensitive information include financial transactions and regulatory actions.
SMTP	Simple Mail Transfer Protocol	A protocol for sending Email messages between servers. SMTP is generally used to send messages from a mail client to a mail server.
	Social Engineering	An attack based on deceiving users or administrators at the target site.
	State Agency	As that term is defined in IC 4-13.1-1-4 and includes any entity that elects to use the services of the IOT.
	Third Party	Someone other than the maker of a machine and the end user. For example, third-party software is software that does not come from the manufacturer of the computer, nor is it developed by the user. Most software today is third-party software.

	Timely	Security issues must be addressed as soon as is feasible by agency staff.
TCP	Transmission Control Protocol	Enables two hosts to establish a connection and exchange streams of data and guarantees delivery of the data and that the packets will be delivered in the same order in which they were sent.
TCP/IP	Transmission Control Protocol/Internet Protocol	The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the *de facto* standard for transmitting data over networks.
URL	Universal Resource Locator	An Internet term which means an address on the World Wide Web. A URL is a string of expressions that can represent any resource on the Internet or local TCP/IP system.
USB	Universal Serial Bus	An external bus standard that supports data transfer rates up to 12 Mbps. USB ports are used to connect peripheral devices, such as mice, modems, and keyboards.
	USB Data Storage Device (aka Flash, jump, pen, or thumb drive)	A small, portable device that plugs into a computer's USB port and functions as a portable hard drive.
	User	A Workforce Member who has authorized access to computer resources.
	UserID	A code which identifies the user.
	Virus	A program or piece of code that is loaded onto a computer system without the user's knowledge with the intent of causing damage, denial of service, or propagating itself across the network.
VPN	Virtual Private Network	A VPN is a software-defined network offering the appearance, functionality, and usefulness of a dedicated private network that is transmitted across a public network. A VPN provides a level of security for data transmission across a Wide Area Network (WAN).
	Volatile Memory	Type of memory whose contents are erased when the system's power is turned off (on interrupted).
	Vulnerability	The absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both.
WAN	Wide Area Network	A common carrier-provided network used to connect LANs and WANs across an extended geographical area - in essence, cities to cities and state to state. This is a way to connect disperse sites for information transmission.
	War Dialing	Dialing telephone numbers in a defined block of numbers looking for computer modem tones.
	War Driving	Locating wireless LAN access points by driving or walking within a defined area.
	Workforce Member	All employees, managers, contractors, interns, volunteers and others who are authorized to access Information Resources to provide government services in State Agencies.

WORM	Write Once, Read Many	An optical disk that allows you to write data onto a disk just once. The data is then permanent and can be read any number of times.